#2

S/N unknown

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Ning SHEN	Serial No.:	unknown
Filed:	concurrent herewith	Docket No.:	9548.63US01
Title:	IDENTITY CREDENCE AND METHOD FOR PRODUCING THE SAME		

CERTIFICATE UNDER 37 CFR 1.10
'Express Mail' mailing label number: EL920772365US
Date of Deposit: 20 July 2001
I hereby certify that this correspondence is being deposited with the United States Postal Service 'Express Mail Post Office To Addressee' service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C . 20231.

By: Omesh Singh
Name: Omesh Singh

SUBMISSION OF PRIORITY DOCUMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

The Applicant encloses herewith one certified copy of a Chinese application, Serial No. 00126213.0, filed 24 August 2000, the right of priority of which is claimed under 35 U.S.C. § 119.

Respectfully submitted,

MERCHANT & GOULD P.C.
P.O. Box 2903
Minneapolis, Minnesota 55402-0903
(612) 332-5300

Dated: 23 July 2001

By: _____
Michael D. Schumann
Reg. No. 30,422

MDS/kjr

证　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：2000 08 24

申　请　号：00 1 26213.0

申请类别：发明专利

发明创造名称：身份证明及其制作方法

申　请　人：杭州中正生物认证技术有限公司

发明人或设计人：沈宁

中华人民共和国
国家知识产权局局长　姜颖

2000 年 10 月 25 日

00.08.28

权 利 要 求 书

1. 一种制作身份证明的方法，其特征在于，包括以下步骤：

构造第一信息包，所述第一信息包包括身份信息和生物信息；

选择一种非对称密钥算法，用私钥对所述第一信息包进行数字密押，生成第二信息包；以及

将密押生成的所述第二信息包存储在一媒体中，制成所述身份证明。

2. 如权利要求 1 所述的身份证明，其特征在于，用私钥对第一信息包进行数字密押的所述步骤包括用所述私钥对所述第一信息包进行加密，形成述第二信息包，而所述第二信息包包括加密后的第一信息包。

3. 如权利要求 1 所述的身份证明，其特征在于，用私钥对第一信息包进行数字密押的所述步骤包括用所述私钥对所述第一信息包进行数字签名，形成第二信息包，而所述第二信息包包括所述第一信息包和所述数字签名。

4. 一种身份证明，其特征在于，包括：

存储媒体，所述存储媒体上存储了用一种非对称密钥算法的私钥对第一信息包进行数字密押而生成的第二信息包，其中第一信息包包括身份信息和生物信息。

5. 如权利要求 4 所述的身份证明，其特征在于，所述第二信息包包括用所述私钥对第一信息包进行加密而生成的信息。

6. 如权利要求 4 所述的身份证明，其特征在于，所述第二信息包括第一信息包和用所述私钥对第一信息包进行数字签名而生成的数字签名。

7. 如权利要求 1 或 4 所述的身份证明，其特征在于，所述生物信息是指纹信息、眼虹膜信息、眼底信息或者掌纹信息。

8. 如权利要求 1 或 4 所述的身份证明，其特征在于，所述非对称密钥算法是 RSA 算法、Pohlig-Hellman 算法、Rabin 算法、ElGamal 算法或者 PGP 算法。

9. 如权利要求 1 或 4 所述的身份证明，其特征在于，所述媒体是 IC 卡、磁盘，或者网络数据库。

10. 如权利要求 1 或 4 所述的身份证明，其特征在于，所述生物信息包含多个信息模板。

00.08.25

6

说　明　书

身份证明及其制作方法

本发明涉及信息加密和认证技术，尤其涉及一种包含数字生物信息的身份证明及其制作方法。

目前在中国，由公安部向公民发放居民身份证。身份证上包含持证人的各种信息，诸如肖像、姓名、性别、民族、出生日期、住址、签发日期、有效期限、编号以及发证机关等。这些信息都是人可读的原始信息，直接反映了持证人的身份。信息的可读性和直观性给身份认证带来了方便。具体地说，当验证身份时，只需将身份证上的肖像与持证人对照。如果面像一致，那么身份证上的信息即代表了持证人的身份。但是，这种身份证很容易被伪造和冒用。例如，通过更改身份证上诸如姓名、出生日期或住址等等任何一个文字和数字信息可以伪造新的身份证。而由于身份验证时全凭主观判断肖像是否与持证人一致，所以如果持证人与身份证上的肖像非常相象，那么他就很容易冒用这份身份证。

为了克服上述身份证容易被伪造和冒用的缺点，已有建议将身份信息通过数字处理存储在智能卡上。但是由于需要使用智能卡，所以这种身份证的制作成本较高。

本发明的一个目的在于提供一种低成本的、不易被伪造和冒用的身份证明。

本发明的另一个目的在于提供一种用于制作上述身份证明的方法。

依照本发明的一个方面，提供了一种制作身份证明的方法，该方法包括以下步骤：构造第一信息包，第一信息包包括身份信息和生物信息；选择一种非对称密钥算法，用私钥对第一信息包进行数字密押，生成第二信息包；以及将密押生成的第二信息包存储在一媒体中，制成身份证明。

依照本发明的另一个方面，提供了一种身份证明，它包括一存储媒体，存储媒体上存储了用一种非对称密钥算法的私钥对第一信息包进行数字密押而生成的第二信息包，其中第一信息包包括身份信息和生物信息。

由于本发明在身份证明制作过程中，选用一种非对称密钥算法，加密和解密所用的密钥不同，而且这两个密钥无法相互推导，所以经私钥数字密押而得到的

第二信息包是一个完整的整体，无法修改，无法拆分，无法拼接。

依照本发明，在制作身份证明时，用于密押的私钥只有发证机关已知，而在对身份证明验证时，终端验证机要对第二信息包进行数字认证，即确认第二信息包是否为发证机关用所述私钥进行密押而得到的，所以任何人无法伪造此身份证明。

另外，在对身份证明验证时，终端验证机要对第二信息包进行生物信息认证，所以任何人无法冒用他人的身份证明。

本发明身份证明的存储媒体可以采用普通的内存式 IC 卡，与现有的智能卡身份证相比，可以大大降低成本。

另外，本发明的身份证明可以随意复制，不会影响其安全性。

下面结合附图，详细描述本发明，其中：

图 1 是一流程图，示出了依照本发明制作身份证明的过程。

图 2 是一流程图，示出了对本发明身份证明进行认证的过程。

首先，说明依照本发明制造身份证明的过程。

如图 1 所示，在步骤 S10，由发证机关为身份证明申请人构造一个个人信息包。该个人信息包包括两类信息，一类是身份信息，例如姓名、性别、民族、出生日期、住址、发证日期、有效期限、编号，以及发证机关等，另一类是生物信息，例如指纹、眼虹膜、眼底、掌纹等。在步骤 S12，发证机关采用非对称密钥算法，用一私钥对个人信息包进行数字密押，生成第二信息包。例如，数字密押可以通过数字加密和数字签名来实现。当用私钥对个人信息包进行数字加密时，第二信息包即是对个人信息包加密后得到的信息。当用私钥对个人信息包进行数字签名时，第二信息包包括个人信息包以及数字签名两者。在步骤 S14，将密押生成的第二信息包存储在一媒体中，完成身份证明的制作。

在本发明的较佳实施例中，非对称密钥算法可以是 RSA（Rivest-Shamir-Adleman）算法。所谓数字密押可以通过数字加密或数字签名来实现。而用于存储第二信息包的媒体可以是 IC 卡、软盘，或网络数据库等。

接下来，参照图 2，说明对本发明身份证明的认证过程。在步骤 S20，用身份证明验证机读取存储在媒体上的第二信息包。在步骤 S22，验证机用一公钥对第二信息包解密。在步骤 S24，认证第二信息包是否为发证机构用上述私钥进行

数字加密或数字签名获得的。如果认证结果是否定的，那么过程进至步骤 S26，将“此身份证明是伪造的”显示在验证机的显示屏上，或者发出一报警声，表示身份证明是伪造的。然后，认证过程结束。如果步骤 S24 的认证结果是肯定的，那么过程进至步骤 S28，验证机读取持证人自身的生物信息，例如指纹、眼虹膜、眼底或掌纹等。在步骤 S30，将验证机读取的生物信息的特征与第二信息包解密后所获得的生物信息的特征进行比较，判断两组生物信息是否一致。如果两组生物信息一致，那么过程进至步骤 S32，将“认证合格”显示在验证机的显示屏上，过程结束。如果两组生物信息不一致，那么过程进至步骤 S34，将“此身份证明被冒用”显示在验证机的显示屏上，或者发出一报警声，表示身份证明被冒用。然后，认证过程结束。

显然，在上述身份证明验证过程中，数字认证和生物信息认证的次序可以互换。

为了更清楚地说明本发明，下面例举两个较佳实施例。

实施例 1：IC 卡指纹身份证

本实施例是将本发明的身份证明应用于身份证。下表列出了公安部为每个公民构造的个人信息包，其中生物信息包含了右手四个手指的指纹信息。

身份信息

信息项	信息内容	存储空间
姓名	10 个汉字	20 字节
性别	用 1 或 0 表示男或女	1 字节
民族	用 1—56 表示 56 个民族	1 字节
出生日期	8 个数字	4 字节
住址	25 个汉字	50 字节
签发日期	8 个数字	4 字节
有效期	8 个数字	4 字节
编号	24 个数字	存储 24 字节
发证机关	20 个汉字	40 字节
卡号	20 个数字	20 字节

指纹信息

信息项	信息内容	存储空间
指纹模板 1	右手食指指纹	256 字节
指纹模板 2	右手中指指纹	256 字节
指纹模板 3	右手无名指指纹	256 字节
指纹模板 4	右手小指指纹	256 字节

公安部选用 RSA 算法，用私钥 A 对上述个人信息包进行数字签名，生成第二信息包。这时第二信息包包括上述个人信息包和数字签名两者。然后，将第二信息包存入内存式 IC 卡内，制成 IC 卡指纹身份证，签发给公民。

持证公民在使用本发明制作的身份证时，需要将身份证插入脱机式 IC 卡指纹身份证验证机中，并且将右手的四个手指按放在验证机的指纹读出部上。验证机用公钥 B 对 IC 卡中存储的第二信息包进行数字签名认证，并且用指纹读出部读出的指纹信息对第二信息包中的指纹信息进行指纹认证。如果数字签名认证和指纹认证都合格，那么持证人的身份得以验证。

上述 IC 卡指纹身份证具有以下优点：

第一，由于在身份证制作过程中，公安部选用的加密 RSA 算法是一种非对称密钥算法，加密密钥 A 和解密密钥 B 不同，而且 A 和 B 无法相互推导，所以经私钥数字签名而得到的第二信息包是一个完整的整体，无法修改，无法拆分，无法拼接。

第二，由于 RSA 算法的私钥只有公安部已知，并且在身份证验证时，脱机式 IC 卡指纹身份证验证机要对第二信息包进行数字签名认证，即确认第二信息包是否为公安部用私钥 A 进行数字签名而得到的，所以任何人无法伪造身份证。

第三，在身份证验证时，脱机式 IC 卡指纹身份证验证机要对第二信息包进行指纹认证，所以任何人无法冒用他人的身份证。

第四，由于采用普通的内存式 IC 卡作为存储媒体，所以成本低，与现有的智能卡身份证相比，大大降低了成本。

第五，这种身份证可以随意复制，不会影响其安全性。

第 2 实施例：工作证

本实施例是将本发明的身份证明应用于单位工作证。下表列出了公司人事部为每个职工构造的个人信息包，其中生物信息包含了右手四个手指的指纹信息。

身份信息

信息项	信息内容	存储空间
姓名	20 个字母	20 字节
性别	用 1 或 0 表示男或女	1 字节
职位	20 个字母	20 字节
出生日期	8 个数字	4 字节
住址	50 个字母	50 字节
签发日期	8 个数字	4 字节
有效期	8 个数字	4 字节
编号	24 个数字	24 字节
发证单位	40 个字母	40 字节
卡号	20 个数字	20 字节

指纹信息

信息项	信息内容	存储空间
指纹模板 1	右手食指指纹	256 字节
指纹模板 2	右手中指指纹	256 字节
指纹模板 3	右手无名指指纹	256 字节
指纹模板 4	右手小指指纹	256 字节

公司人事部选用 RSA 算法，用私钥 A 对上述个人信息包进行加密，生成第二信息包。这时第二信息包即是对上述个人信息包加密后得到的信息。然后，将第二信息包存入磁盘中，制成工作证。

公司职员在使用本发明制作的工作证时，可以将工作证磁盘插入电脑中，并且将右手的四个手指按放在与电脑相连的指纹读出器上。电脑用公钥 B 对磁盘中

存储的第二信息包进行数字认证，并且用指纹读出器读出的指纹信息对第二信息包中的指纹信息进行指纹认证。如果数字认证和指纹认证都合格，那么持证人的身份得以验证。

本发明的工作证也具有上述 IC 卡指纹身份证的优点。

本领域的熟练技术人员应该明白，尽管在较佳实施例中，身份证明的载体为 IC 卡或磁盘，但本发明不限于此。发证机关还可以将第二信息包存储在网络数据库等媒体上，为携带和传输提供方便。尽管在较佳实施例中，发证机关用 RSA 算法对个人信息包进行加密或数字签名，但本发明不限于此。发证机关还可以使用诸如 Pohlig-Hellman 算法、Rabin 算法、ElGamal 算法或者 PGP 算法等其它形式的非对称密钥算法进行加密。另外，个人信息包中的信息项可以按需要增加和减少，信息内容和存储空间也可以按需要进行变化。生物信息不限于指纹，它还可以是眼虹膜、眼底或掌纹等。在本发明的较佳实施例中，生物信息包括 4 个指纹模板，但本发明的模板数目不限于此。发证机关可以只采用一个指纹模板。只是在这种情况下，如果持证人的相应手指受伤，无法获得指纹特征时，指纹认证就会出现问题。使指纹信息包含多个指纹模板可以在某个手指受伤或受损的情况，仍能用剩余的指纹模板进行指纹认证。当把眼虹膜、眼底或掌纹等用作生物信息时，同样可以采用一个或多个信息模板。

本领域的熟练技术人员应该认识到，在不脱离本发明范围和精神的情况下，可以对本发明的实施例进行任何变化。本发明要求保护的范围由后附的权利要求书来限定。

说 明 书 附 图

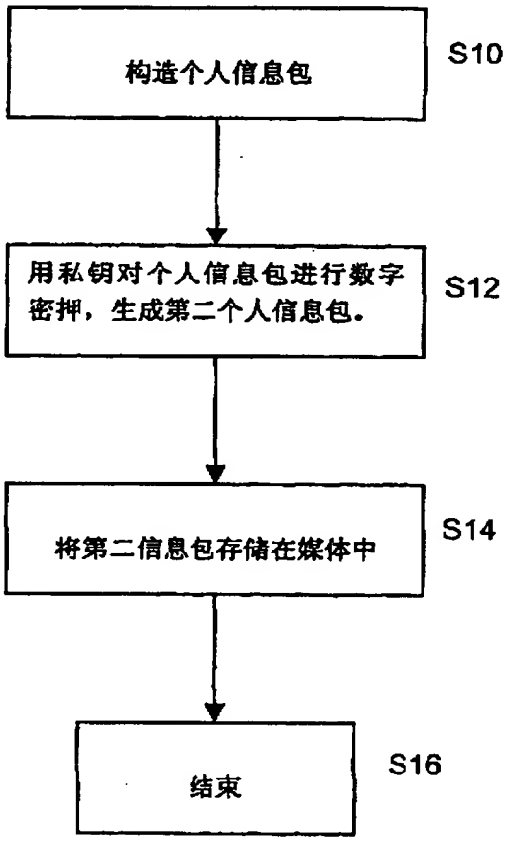
构造个人信息包
S10
用私钥对个人信息包进行数字密押，生成第二个人信息包。
S12
将第二信息包存储在媒体中
S14
结束
S16

图 1

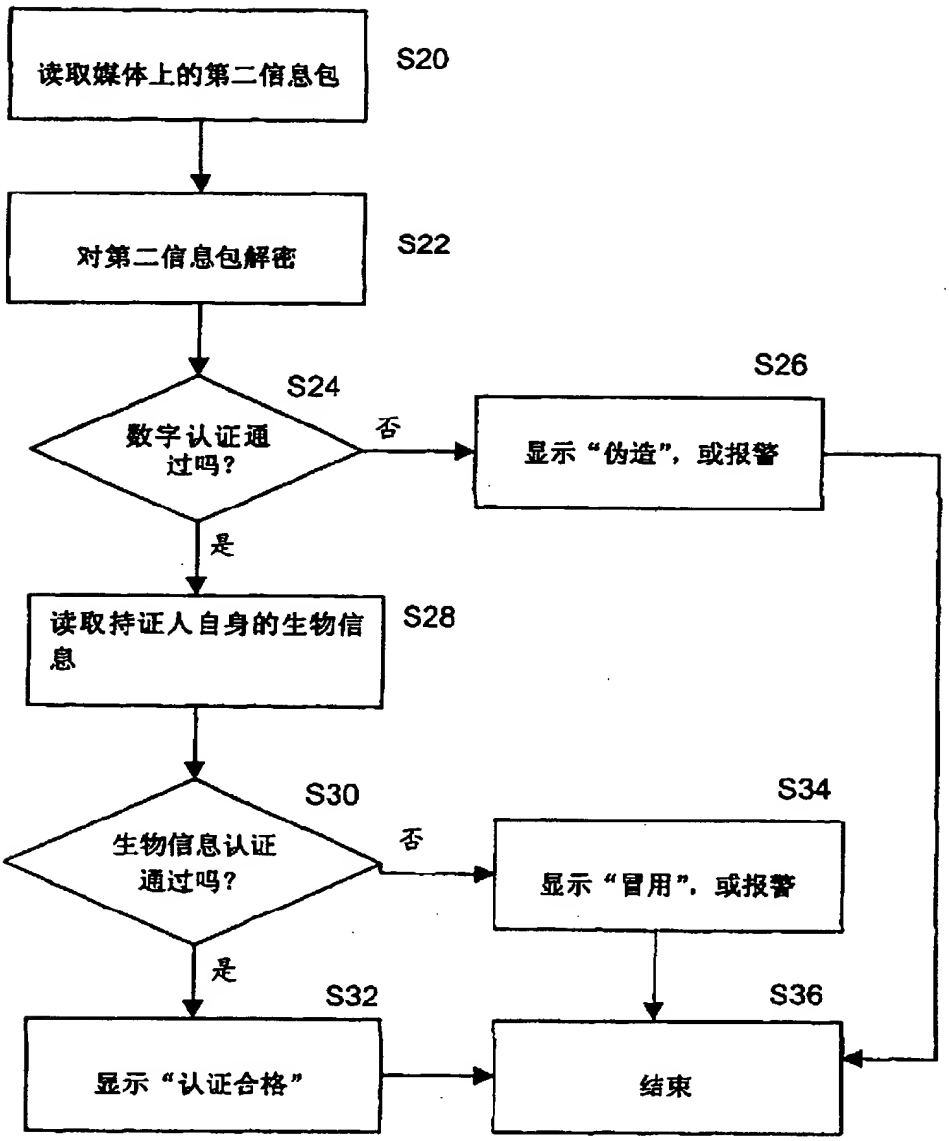
读取媒体上的第二信息包
S20
对第二信息包解密
S22
S24
数字认证通过吗？
否
S26
显示“伪造”，或报警
是
读取持证人自身的生物信息
S28
S30
生物信息认证通过吗？
否
S34
显示“冒用”，或报警
是
S32
显示“认证合格”
S36
结束

图 2